SIR IUS 5/16

SLOVENSKI INŠTITUT za REVIZIJO

Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Dr. Boštjan Delak

Izzivi revizorjev informacijskih sistemov pri dajanju zagotovil pri logičnih dostopih

The information systems auditors' issues at the logical access audit assurance activities

POVZETEK ● *Eden najpomembnejših gradnikov pri varovanju informacij za učinkovito ter varno uporabo informacijskih sistemov so ustrezni dejavniki prepoznavanja uporabnika ob dostopu do informacijskega sistema ter učinkovita uporaba ustreznih varnostnih ukrepov za kontrole upravljanja in nadzora uporabniškega dostopa. Vendar se moramo zavedati, da je najpomembnejši in morda tudi najšibkejši člen človek – uporabnik informacijskih sistemov. Prispevek seznani bralca z dejavniki prepoznavanja neprivilegiranega uporabnika ter predstavi pomembne standarde, metodologije in dobre prakse na tem področju.*

V pregledu literature so predstavljeni nekateri strokovni in znanstveni prispevki o tej temi. V prispevku so predstavljene tudi izkušnje iz dajanja zagotovil na tem področju v Sloveniji ter nekatere možne aktivnosti v zvezi z njihovim izvajanjem. Revizorji informacijskih sistemov moramo biti pri dajanju zagotovil, pri revizijah, pregledih in dogovorjenih postopkih pozorni na nepravilnosti in nezakonita dejanja. Posojanje gesel spada med nepravilnosti in predstavlja varnostne incidente ter kršitev varovanja informacij. S temi izzivi se lahko srečujemo na vseh področjih: dejavnosti posameznih organizacij, kjer so dostopi do podatkov v informacijske sisteme zaščiteni z uporabniškimi imeni in gesli. Prispevek revizorje informacijskih sistemov opozarja na te nepravilnosti in pojasnjuje načine prepoznavanja teh dejanj in zmanjševanja tveganj.

Ključne besede ● *geslo, osebni identifikator, prepoznavanje, dostop do informacijskih sistemov, tveganja, posojanje gesel*

SUMMARY ● *One of the most important building blocks of information security in an effective and secure use of information systems is the relevant identification of the user having access to the information system. Information security must provide effective use of appropriate safety measures for the control of the management and of user access. However, we must be aware that the most important and perhaps the weakest link within the information system are people – the information system users. The paper acquaints the reader with the elements identifying the user, and presents some important standards, methodologies and best practices in this field. The literature review presents some technical and scientific input on this topic. The paper also presents the experience of assurances in this area in Slovenia, and some possible activities for providing them. Information systems auditors have to provide assurance in audits, reviews and agreed-*

upon procedures and should pay attention to irregularities and illegal acts. Lending passwords are one of the irregularities constituting security incidents and violation of information security. Such challenges may be encountered in all areas of activities of individual organizations, where the access to data in the information systems is protected by usernames and passwords. The contribution of information system auditors draws attention to these irregularities and explains how to identify them and reduce the risks.

Key words ● *password, personal identifier, identification, access to information systems, risk, lending passwords*

Maja Hmelak

Razumevanje informacijskega okolja v reviziji računovodskih izkazov: spoznavanje informacijskega okolja in splošne kontrole

General Risk and Internal Control in Financial Auditing

POVZETEK ● *Razumevanje vloge informacijskega okolja ima pomembno vlogo v revidiranju računovodskih izkazov. V pričujočem prispevku bomo predstavili vlogo spoznavanja informacijskega okolja revidiranih organizacij in razumevanja splošnih tveganj in kontrol v fazi ocenjevanja tveganj – revizijsko aktivnost, ki jo finančni revizorji pogosto prepustijo strokovnjakom za področje informacijskih tehnologij, na primer revizorjem informacijskih sistemov. V prihodnjem prispevku bomo predstavili vlogo razumevanja avtomatiziranih notranjih kontrol, ki jih revizorji računovodskih izkazov praviloma presojajo v okviru ocenjevanja tveganj na ravni organizacijskih procesov.*

Ključne besede ● *MSR, informacijsko okolje, splošne kontrole informacijskega okolja, avtomatizirane notranje kontrole*

SUMMARY ● *Understanding the organization's information environment plays an increasingly important role in financial auditing. This article highlights the importance of understanding the information systems in the companies under audit and the thereto related risks in the risk assessment phase of a financial audit – an activity, frequently outsourced to IT specialists, e.g. IT auditors. In a future financial-audit-focused edition of SIR*IUS, this topic will continue with an article on understanding the functioning of automated internal controls in organizations.*

Key words ● *IAS, information system enviroment, general computer controls, autimated internal controls*

Igor Karnet

Digitalizacija poslovanja bank

Digital Business in banks

POVZETEK ● *Potrošniki in komitenti vedno glasneje povprašujejo ali celo zahtevajo razne e-storitve, ki bi jim prihranile čas, povečale učinkovitost in izboljšale uporabniško izkušnjo. Zato so podjetja, banke in druge organizacije primorane razvijati nove storitve in produkte ter jih skupaj z že obstoječimi ponujati tudi preko digitalnih prodajnih kanalov. Le tako lahko ohranijo sloves sodobne organizacije. Biti sodoben ali celo vodilni v svoji panogi, prinese konkretne koristi, priložnosti, prednosti in povečan ugled, na drugi strani pa tudi obveznosti, odgovornosti, zaveze in tveganja. Povečan obseg digitalnega poslovanja ne zadeva samo uporabnikov storitev, ampak tudi zaposlene. Pri tem je treba najti ravnovesje med ponujenimi storitvami in funkcionalnostmi ter upravljanjem raznih IT- in drugih tveganj, ki jih je treba pravočasno zaznati oz. predvideti in se nanje primerno pripraviti in odzivati – tako v času normalnega delovanja kot tudi v času izrednega dogodka.*

V prispevku bodo predstavljene ključne grožnje ter tudi nasveti, kako se digitalizacije poslovanja uspešno in varno lotiti.

Ključne besede ● *digitalizacija, poslovanje, tveganje, priložnosti, koristi*

SUMMARY ● *Customers and clients increasingly demand or even require all kinds of e-services that would save their time, increase their efficiency and improve the user experience. Therefore, companies, banks and other organizations are forced to strive for the development of new services and products and, together with existing ones, offer them via digital channels. That is the only way to preserve the reputation of a modern organization. Being modern, or even an industry leader, brings concrete benefits, opportunities, advantages and increased prestige, as well as obligations, responsibilities, commitments and risks. Increased volume of digital business does not only concern the users of those e-services, but also employees. It is necessary to find the right mix of e-services and functionalities offered and on the other side of management of various IT and other risks, which need to be detected in a timely manner – both during normal operation as well as during non-desired situations.*

The paper will present key threats, as well as advice on how successfully and safely to approach the digitization of business.

Key words ● *digitization, business, risks, opportunities, benefits*

Kristjan Košič, Saša Kuhar, Katja Kous, Tina Schweighofer

Standardi in dobre prakse s področja razvoja medicinske programske opreme

Standards and guidance documents for medical software development

POVZETEK ● *V okviru razvoja medicinske programske opreme je treba posvetiti pozornost ključnim zahtevam medicinske direktive – Aneksu I dokumenta (European Council, 1993) in jim slediti skozi vse korake življenjskega cikla razvoja medicinske programske opreme (ISO/IEC 62304:2006, 2006). Pomembno je, da upoštevamo domensko specifične standarde ter priporočila, pri čemer nikakor ne smemo spregledati področja zagotavljanja kakovosti (ISO/IEC 13485:2016, 2016) in upravljanja tveganj (ISO/IEC 14971:2007, 2007), saj gre za razvoj življenjsko kritičnega informacijskega sistema. V prispevku bomo pregledali osnovne standarde, ki vključujejo proces razvoja medicinske programske opreme, jih povezali s ključnimi zahtevami medicinske direktive in upravljanjem tveganj ter opisali minimalno vsebino osnovne tehnične mape, ki jo mora imeti na voljo vsak medicinski pripomoček. Vsebina mape je osnova za certifikacijo in tudi revizijski postopek.*
Ključne besede ● *medicinska programska oprema, tveganja, revizija, življenjski cikel razvoja programske opreme*

SUMMARY ● *In medical software development, special attention needs to be devoted to the essential requirements of the Medical Devices Directive, Annex I (European Council, 1993), which have to be followed through all the stages of the development cycle and the production process of the devices (ISO/IEC 62304:2006, 2006). Specific standards and recommendations have to be observed, both in terms of quality (ISO/IEC 13485:2016, 2016) and risk management (ISO/IEC 14971:2007, 2007) in the development of this vital information system. The article gives a survey of the basic standards included in the process of medical software development life cycle and combines them with the essential requirements of the Medical Devices Directive and the risk management involved. It is followed by a description of the minimum information contained the basic technical file accompanying each and every medical device, which is then the basis for certification and audits.*
Key words ● *medical device software, risk management, software development life cycle*

Vesna Štager

Prihodki nadzorne institucije in sankcioniranje kršitev v revizijski stroki v Nemčiji, Avstriji in Sloveniji

Revenues of supervisory institutions and sanctions for violations in Audit Profession in Germany, Austria and Slovenia

POVZETEK ● *Države članice EU so morale do 17. 6. 2016 v svojo zakonodajo vključiti Direktivo 2014/56/EU o obveznih revizijah za letne in konsolidirane računovodske izkaze. Od takrat članice zavezuje tudi Uredba (EU) 537/2014 o posebnih zahtevah v zvezi z obvezno revizijo subjektov javnega interesa. V članku predstavljam izvršitev prava Direktive EU in uporabo določb Uredbe za področje revidiranja v Nemčiji, Avstriji in*

Sloveniji, kjer smo se omejili na področje prihodkov oziroma financiranje nadzorne institucije in sankcioniranje kršitev. Poudarek je na primerjalni analizi vrst in višine sankcij.
Ključne besede ● *Direktiva EU za revizijo, reforma revizijskega trga*

SUMMARY ● *EU*[1] *Member States were required by 17 June 2016 to include in their legislation the Directive 2014/56/EU on Statutory Audits of Annual Accounts and Consolidated Accounts. From the same day, the States are also bound by Regulation (EU) 537/2014 on specific requirements regarding the statutory audit of public-interest entities. The paper presents the enforcement of the EU law Directive and the application of the provisions of the scope of the audit in Germany, Austria and Slovenia, where we have limited scope: Revenues of supervisory institutions and sanctions for violations. The focus is on the comparative analysis of types and levels of sanctions.*
Key words ● *EU Directive on Statutory Audits, reform of the audit market*

[1] The responsible translator for the English language is mag. Shelagh Hedges (native speaker), University of Maribor.